REMARKS

Claims 1-9, 11-24, 26-42 and 44-56 are pending. Claims 1, 19 and 39 have been amended for clarity, without acquiescence or prejudice to pursue the original claims in a related application. No new matter has been added.

Claim 1 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,178,511 (Cohen) in view of U.S. Patent No. 6,158,010 (Moriconi), and U.S. Patent Application Publication No. 2001/0023440 (Franklin). Claims 19-38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cohen in view of Moriconi, Franklin, U.S. Patent Application Publication No. 2002/0082818 (Ferguson), and U.S. Patent Application Publication No. 2002/0026592 (Gavrila). Claim 39 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Cohen in view of Moriconi, Franklin, and Gavrila.

Claims 1 and 39 have been amended to recite receiving the user role at a local database network node from the central directory; determining a local policy having user privileges for the local database network node, wherein the local policy is determined by locally processing the user role that is at the central directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the central directory. Claim 19 has been amended to recite wherein the one or more local database network nodes determines a local policy having the privilege for the local database network node, wherein the privilege is determined by locally processing the one of the collection of roles from the LDAP directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the LDAP directory.

Thus, the claimed invention includes two tier authorizations. At the global level there is user role authorization. At the local level, there is privilege granting using the local policy based on the user role. The local policy for each local database network node may be different between the different local database network nodes associated with the same directory sharing the same user role information.

As such, claims 1, 19 and 39 includes the feature of locally processing the role that is at the directory (locally), wherein the act of locally processing is performed at the local database

network node that is one of the one or more database network nodes that is associated with the directory (globally).

Applicant respectfully submits that Moriconi does not disclose or suggest the above feature. In particular, column 4, lines 19-33 of Moriconi discloses:

> In the preferred embodiment, the system comprises a policy manager located on a server for managing and distributing a local client policy based on a global security policy, and an application guard located on a client or server associated with one or more clients for managing access to securable components as specified by the local client policy. The global policy specifies access privileges of the user to securable components. The policy manager may then distribute a local client policy based on the global policy to the client or server. An application guard located on the client or server then manages authorization requests to the securable components as specified by the local client policy. Each authorization request may be recorded in an audit log to keep track of the authorization requests, whether they were granted or denied, and other useful information.
>
> (Emphasis Added)

As such, Moriconi discloses a "global" security policy that centrally manages access privileges, and does not disclose or suggest locally determining at the local database network node a user role that is at the central directory (wherein the act of locally associating is performed at one of the network nodes that is associated with the central directory), nor does Moriconi disclose or suggest a privilege that is locally defined at one of the one or more database network nodes based on role information from the global directory. Also, since Moriconi specifically requires that privileges and policies for local network nodes be centrally managed by the "global" security policy, Moriconi in fact teaches away from locally determining and interpreting at a network node a privilege based on a user role, and from locally defining a privilege/policy at a database network node. Moriconi merely uses a policy from the global level and enforces that policy at a local level.

Cohen, Franklin, and Gavrila also do not disclose or suggest the above feature, and therefore, fail to make up the deficiencies present in Moriconi. Since none of the cited references discloses or suggests the above featre, they cannot be combined to form the resulting subject matter of claims 1, 19, and 39. For at least the foregoing reason, claims 1, 19, and 39,

and their respective dependent claims, are believed allowable over the cited references and their combination.

CONCLUSION

On the basis of the above remarks, reconsideration and allowance of the claims is believed to be warranted and such action is respectfully requested. If the Examiner has any questions or comments, the Examiner is respectfully requested to contact the undersigned at the number listed below.

The Commissioner is authorized to charge any fees due in connection with the filing of this document to Bingham McCutchen's Deposit Account No. **50-4047,** referencing billing number **7010852003.** The Commissioner is authorized to credit any overpayment or to charge any underpayment to Bingham McCutchen's Deposit Account No. **50-4047,** referencing billing number **7010852003.**

Respectfully submitted,

Dated: October 22, 2007

By: _____
Jasper Kwoh
Reg. No. 54,921

Bingham McCutchen LLP
Three Embarcadero Center
San Francisco, CA 94111-4067
Telephone: (650) 849-4400
Telefax: (650) 849-4800